PATENT ABSTRACTS OF JAPAN

(51)Int.Cl.   HO4L   9/08
                                     G09C   5/00
                                     HO4L   9/00
                                     HO4L   9/32

(21)Application number : 2002-028915   (71)Applicant : SONY CORP

(22)Date of filing :   06.02.2002   (72)Inventor : TANAKA KOICHI
                                                        KAWAKAMI TATSU
                                                        KURODA HISASUKE
                                                        ISHIGURO RYUJI

(30)Priority

Priority number : 2001033114   Priority date : 09.02.2001   Priority country : JP
                 2001094803   29.03.2001   JP

(54) INFORMATION PROCESSOR AND METHODLICENSE SERVERAND PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To freely distribute contents and allow only authorized
users to utilize the contents.

SOLUTION: A client receives an encrypted content from a content server. The
header of the content includes license-identifying information for identifying a license
required in utilization of the content. The client requests a license server to transmit
a license identified by the license-identifying information. When receiving the request
for a licensethe license server carries out a charging process before transmitting the
license to the client. The client can decode and play back the content on the
condition of possessing the license.

CLAIMS

[Claim(s)]
[Claim 1]An information processor comprising:
License specific information for specifying said license which carries out the utilization permission of the contents concerned in an information processor which permits use of contents on condition that a license is held.
Enciphered contents data.
A content storing means which memorizes said contents including key information required in order to decode contents data.
A license memory measure which memorizes a license containing contents specific information for specifying said contents by which a utilization permission is carried outA judging means which judges whether a license which can carry out the utilization permission of said contents is memorized by said license memory measureand a decoding means which decodes contents data of said contents on condition that it was judged that a license was memorized by said judging means.

[Claim 2]The information processor according to claim 1 which is provided with the following and characterized by a license received by said reception means being memorized by said license memory measure.
A transmitting means which transmits a license request containing license identification information for said information processor to identify a license to a license server further.
A reception means which receives a license transmitted by license server.

[Claim 3]The information processor according to claim 1wherein said contents data is further provided with a reproduction means which reproduces contents data which is the data which combined text dataimage datavoice dataa video dataor themand was decoded by said decoding means.
[Claim 4]Said key information contains EKB (Enabling Key Block)Said information processor is provided with a device node key memory measure which memorizes a device node key furtherSaid decoding means said EKB (Enabling Key Block) using a route key by which decoding processing might be carried out using said device node key memorized by said device node key memory measure said enciphered contents data. The decoding information processor according to claim 1.
[Claim 5]Said key information contains a contents key further enciphered by route key of said EKB (Enabling Key Block)Said contents data is enciphered by said contents keySaid decoding means said contents key decoded using a route key by which decoding processing might be carried out in said EKB (Enabling Key Block) using said device node key memorized by said device node key memory measure. The information processor according to claim 4 using and decoding said enciphered contents data.
[Claim 6]The information processor according to claim 1wherein said license includes

service-condition information which shows further a service condition of contents which become available according to the license concerned.
[Claim 7]The information processor according to claim 1wherein said license includes further an electronic signature made with a secret key of a license server.
[Claim 8]Said information processor is provided with a terminal-identification-information memory measure which memorizes terminal identification information which identifies an information processor furtherSaid license request includes further said terminal identification information memorized by terminal-identification-information memory measureFurther said license received by said reception means including said terminal identification information said judging meansSaid terminal identification information included in said license is compared with said terminal identification information memorized by said terminal-identification-information memory measureThe information processor according to claim 2 restricting when both are in agreementand judging that the license concerned is a license to which use of said contents is permissible.
[Claim 9]An information processing method with which use of contents is permitted on condition that a license characterized by comprising the following is held.
License specific information for specifying said license which carries out the utilization permission of the contents concerned.
Key information required in order to decode enciphered contents data and contents data.

[Claim 10]License specific information for being a program which makes a computer perform processing to which use of contents is permitted on condition that a license is heldand specifying said license which carries out the utilization permission of the contents concernedEnciphered contents data and key information required in order to decode contents dataA step which memorizes a license containing contents specific information for specifying a step which memorizes ***** contentsand said contents a utilization permission is carried out by the license concerned ofA step which judges whether a license which can carry out the utilization permission of said contents is memorized by said license memory measureA program which makes a computer perform a step which decodes contents data of said contents on condition that it was judged that a license was memorized by said judging means.
[Claim 11]The program according to claim 10wherein said program or its part is enciphered.
[Claim 12]In a license server which publishes a license to which use of contents is permittedContents specific information for specifying said contents a utilization permission is carried out by the license concerned ofA reception means which receives a license request containing license identification information which was transmitted from a license memory measure which memorizes said license including terminal identification information which identifies an information processorand an

information processorand which identifies a licenseAn extraction means to extract said license corresponding to said license identification information contained in said license request from said license memory measureA processing means to add said terminal identification information to said license extracted by said extraction meansA signature means which adds an electronic signature to a license to which terminal identification information was added by said processing means using a secret key of a license serverA license server provided with a transmitting means which transmits a license signed by said signature means to an information processor which transmitted said license request.

[Claim 13]Contents specific information for being an information processing method which publishes a license to which use of contents is permittedand specifying said contents a utilization permission is carried out by the license concerned ofA step which memorizes said license including terminal identification information which identifies an information processorA step which receives a license request containing license identification information which was transmitted from an information processorand which identifies a licenseA step which extracts said license corresponding to said license identification information contained in said license request from said license memory measureA step which adds said terminal identification information to said license extracted by said extraction meansA step which adds an electronic signature to a license to which terminal identification information was added by said processing means using a secret key of a license serverAn information processing method containing a step which transmits a license signed by said signature means to an information processor which transmitted said license request.

[Claim 14]Contents specific information for being a program which makes a computer perform processing processing which publishes a license to which use of contents is permittedand specifying said contents a utilization permission is carried out by the license concerned ofA step which memorizes said license including terminal identification information which identifies an information processorA step which receives a license request containing license identification information which was transmitted from an information processorand which identifies a licenseA step which extracts said license corresponding to said license identification information contained in said license request from said license memory measureA step which adds said terminal identification information to said license extracted by said extraction meansA step which adds an electronic signature to a license to which terminal identification information was added by said processing means using a secret key of a license serverA program which makes a computer perform a step which transmits a license signed by said signature means to an information processor which transmitted said license request.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention about an information processor and a methoda license serverand a programThe contents which have not been licensed in particular from an owner of a copyright are copied unjustlyand are related with the information processor and the methodlicense serverand program which enabled it to prevent being used.

[0002]

[Description of the Prior Art]These daysas a user provides other users with the music data which he holds via the Internet and offers are received for the music data which he does not hold from other usersthe system where two or more users exchange music data for nothing and which they suit is realized.

[0003]If the contents of one music and others exist theoreticallyin order that other users of all the may be enabled to use it and many users may not purchase contents in such a systemSince the owner of a copyright about contents cannot sell the contents as workshe will lose an opportunity to receive the loyalty about use of the works which can originally be received with sale of works.

[0004]

[Problem(s) to be Solved by the Invention]Thenit is requested socially that it should prevent being used unjustlywithout barring circulation of contents.

[0005]This invention is made in view of such a situationand it enables it to prevent contents from being used unjustly certainly.

[0006]

[Means for Solving the Problem]License specific information for specifying a license required in order that an information processor of this invention may carry out the utilization permission of the contentsA content storing means which memorizes contents including enciphered contents data and key information required in order to decode contents dataA license memory measure which memorizes a license containing contents specific information for specifying contents by which a utilization permission is carried outA judging means which judges whether a license which can carry out the utilization permission of the contents is memorized by license memory measureIt has a decoding means which decodes contents data of contents on condition that it was judged that a license was memorized by a judging means.

[0007]A transmitting means which transmits a license request containing license identification information for an information processor to identify a license to a license server furtherIt has a reception means which receives a license transmitted by license serverand a license received by a reception means can be memorized by license memory measure.

[0008]Contents data is the data which combined text dataimage datavoice dataa

video dataor themand can be further provided with a reproduction means which reproduces contents data decoded by decoding means.

[0009]Key information contains EKB (Enabling Key Block)An information processor is provided with a device node key memory measure which memorizes a device node key furtherThe decoding means can decode contents data enciphered using a route key by which decoding processing might be carried out in EKB (EnablingKey Block) using a device node key memorized by device node key memory measure.

[0010]Key information contains a contents key further enciphered by route key of EKB (Enabling Key Block)Contents data is enciphered by contents keyA decoding means contents data enciphered using a contents key decoded using a route key by which decoding processing might be carried out in EKB (Enabling Key Block) using a device node key memorized by device node key memory measure. It can decode.

[0011]The license can include service-condition information which shows further a service condition of contents which become available according to the license.

[0012]The license can include further an electronic signature made with a secret key of a license server.

[0013]An information processor is provided with a terminal-identification-information memory measure which memorizes terminal identification information which identifies an information processor furtherFurther a license with which a license request was further received by a reception means including terminal identification information memorized by terminal-identification-information memory measure including terminal identification information a judging meansTerminal identification information included in a license is compared with terminal identification information memorized by terminal-identification-information memory measurewhen both are in agreementit restrictsand it can judge that the license is a license to which use of contents is permissible.

[0014]License specific information for an information processing method of this invention to specify a license which carries out the utilization permission of the contentsEnciphered contents data and key information required in order to decode contents dataA step which memorizes a step which memorizes ***** contentsand a license containing contents specific information for specifying contents by which a utilization permission is carried outA step which judges whether a license which can carry out the utilization permission of the contents is memorized by license memory measureA step which decodes contents data of contents on condition that it was judged that a license was memorized by a judging means is included.

[0015]License specific information for a program of this invention to specify a license which carries out the utilization permission of the contentsEnciphered contents data and key information required in order to decode contents dataA step which memorizes a step which memorizes ***** contentsand a license containing contents specific information for specifying contents by which a utilization permission is carried outA step which judges whether a license which can carry out the utilization

permission of the contents is memorized by license memory measureA computer is made to perform a step which decodes contents data of contents on condition that it was judged that a license was memorized by a judging means.

[0016]A program or its part can be enciphered.

[0017]Since contents permitted are specifiedthis invention is characterized by a license server comprising the following.

Contents specific information.

A license memory measure which memorizes a license including terminal identification information which identifies an information processor.

A reception means which receives a license request containing license identification information which was transmitted from an information processorand which identifies a license.

An extraction means to extract a license corresponding to license identification information contained in a license request from a license memory measureA processing means to add terminal identification information to a license extracted by an extraction measureA signature means which adds an electronic signature to a license to which terminal identification information was added by a processing means using a secret key of a license serverand a transmitting means which transmits a license signed by a signature means to an information processor which transmitted a license request.

[0018]Since contents by which a utilization permission is carried out are specifiedthis invention is characterized by an information processing method comprising the following.

Contents specific information.

A step which memorizes a license including terminal identification information which identifies an information processor.

A step which receives a license request containing license identification information which was transmitted from an information processorand which identifies a license.

A step which extracts a license corresponding to license identification information contained in a license request from a license memory measureA step which adds terminal identification information to a license extracted by an extraction measureA step which adds an electronic signature to a license to which terminal identification information was added by a processing means using a secret key of a license serverand a step which transmits a license signed by a signature means to an information processor which transmitted a license request.

[0019]In an information processor of this inventionan information processing methodand a programon condition that a license is heldcontents are decodedand it is made available.

[0020]In a license server of this inventionand an information processing methodan

effective license is published only with a specific information processor.

[0021]

[Embodiment of the Invention]Drawing 1 shows the composition of the contents providing system which applied this invention. Client 1-11-2 (hereafterwhen these clients do not need to be distinguished separatelythe client 1 is only called) is connected to the Internet 2. In this examplealthough two clients are shownthe client of the arbitrary number is connected to the Internet 2.

[0022]On the Internet 2. When the contents server 3 which provides contents to the client 1the license server 4 which gives a license required to use the contents which the contents server 3 provides to the client 1and the client 1 receive a licenseThe fee collection server 5 which performs accounting to the client 1 is connected.

[0023]These contents servers 3the license server 4and the fee collection server 5 are also connected to the arbitrary number and the Internet 2.

[0024]Drawing 2 expresses the composition of the client 1.

[0025]In drawing 2CPU(Central Processing Unit) 21Various kinds of processings are performed according to the program memorized by ROM(Read Only Memory) 22 or the program loaded to RAM(Random Access Memory) 23 from the storage parts store 28. the timer 20 -- a time check -- it operates and time information is supplied to CPU21. To RAM23CPU21 performs various kinds of processings againand also required data etc. are memorized suitably.

[0026]The encryption decoding part 24 performs processing which decodes the already enciphered contents data while enciphering contents data. The codec part 25 encodes contents data by ATRAC(Adaptive Transform Acoustic Coding)3 method etc.for exampleIt is made to supply and record on the semiconductor memory 44 connected to the drive 30 via the input/output interface 32. Or the codec part 25 decodes the data which was read from the semiconductor memory 44 via the drive 30 and which is encoded again.

[0027]The semiconductor memory 44 is constituted by the memory stick (trademark) etc.for example.

[0028]CPU21ROM22RAM23the encryption decoding part 24and the codec part 25 are mutually connected via the bus 31. The input/output interface 32 is also connected to this bus 31 again.

[0029]The input part 26CRT which become the input/output interface 32 from a keyboarda mouseetc.The communications department 29 which comprises the storage parts store 28a modema terminal adopteretc. which comprise the outputting part 27 which consists of a display which consists of LCD etc.a loudspeakeretc.a hard disketc. is connected. The communications department 29 performs the communications processing through the Internet 2. The communications department 29 performs the communications processing of an analog signal or a digital signal among other clients again.

[0030]The drive 30 is connected to the input/output interface 32 again if neededIt is

suitably equipped with the magnetic disk 41the optical disc 42the magneto-optical disc 43or the semiconductor memory 44and the computer program read from them is installed in the storage parts store 28 if needed.

[0031]Although a graphic display is omittedthe contents server 3the license server 4and the fee collection server 5 are also constituted by the client 1 shown in drawing 2and the computer which has the same composition fundamentally. Thenin the following explanationthe composition of drawing 2 is quoted also as composition of the contents server 3the license server 4the fee collection server 5etc.

[0032]Nextwith reference to the flow chart of drawing 3the client 1 explains the processing which receives offer of contents from the contents server 3.

[0033]When a user orders it access to the contents server 3 by operating the input part 26CPU21 controls the communications department 29 and he makes it access the contents server 3 via the Internet 2 in Step S1. In Step S2a user operates the input part 26and if the contents which receive offer are specifiedCPU21 will receive this specification information and will notify the contents specified as the contents server 3 via the Internet 2 from the communications department 29. The contents server 3 which received this notice so that it may mention later with reference to the flow chart of drawing 4Since the enciphered contents data is transmittedin Step S3 CPU21If this contents data is received via the communications department 29that contents data enciphered will be supplied and stored in the hard disk which constitutes the storage parts store 28 in step S4.

[0034]Nextwith reference to the flow chart of drawing 4contents offer processing of the contents server 3 corresponding to the above processing of the client 1 is explained. In the following explanationthe composition of the client 1 of drawing 2 is quoted also as composition of the contents server 3.

[0035]In Step S21CPU21 of the contents server 3It stands by until it receives access from the Internet 2 from the client 1 via the communications department 29and when it judges with having received accessit progresses to Step S22 and the information which specifies the contents transmitted from the client 1 is incorporated. The information which specifies these contents is information which the client 1 has notified in Step S2 of drawing 3.

[0036]In Step S23CPU21 of the contents server 3 reads the contents specified for the information incorporated by processing of Step S22 out of the contents data memorized by the storage parts store 28. CPU21 supplies the contents data read from the storage parts store 28 to the encryption decoding part 24and makes it encipher in Step S24 using the contents key Kc.

[0037]Since the contents data memorized by the storage parts store 28 is already encoded by the codec part 25 with ATRAC3 methodthis contents data encoded will be enciphered.

[0038]Of coursethe storage parts store 28 can be made to memorize contents data in the state where it enciphered beforehand. In this caseprocessing of Step S24 can be

omitted.

[0039]Nextin Step S25 CPU21 of the contents server 3Key information (EKB and K_{EKBC} (Kc) which are later mentioned with reference to <u>drawing 5</u>) required to decode the contents enciphered by the header which constitutes the format which transmits the enciphered contents dataLicense ID for identifying a license required to use contents is added. And in Step S26 CPU21 of the contents server 3The data which formatted the key and the header which added license ID is transmitted to the accessed client 1 via the Internet 2 from the communications department 29 at the contents enciphered by processing of Step S24and processing of Step S25.

[0040]<u>Drawing 5</u> is carried out in this wayand expresses the composition of the format in case contents are supplied to the client 1 from the contents server 3. This format is constituted by header (Header) and the data (Data) as shown in the figure.

[0041]In a headercontents information (Content information)Digital-rights-management information (DRM (Digital Right Management) information)license ID (License ID) and an INEBU ring key block (validation key blocks) (EKB (EnablingKey Block)) -- andData K_{EKBC} (Kc) as the contents key Kc enciphered using key K_{EKBC} generated from EKB is arranged. EKB is later mentioned with reference to <u>drawing 15</u>.

[0042]Informationincluding the method etc. of the content ID (CID) as identification information for identifying the contents data by which formatting is carried out as dataand the codec of the contentsis included in contents information.

[0043]The rule and state (Usagerules/status) which use contents for digital-rights-management informationand URL (Uniform Resource Locator) are arranged. The reproduction frequency of contentscopy frequencyetc. are described by a use rule and the statefor example.

[0044]URL is address information accessed when acquiring the license specified by license IDand is an address of the license server 4 specifically required in the case of the system of <u>drawing 1</u>since it is licensed. License ID identifies the license needed when using the contents currently recorded as data.

[0045]Data is constituted by arbitrary numbers of encryption blocks (Encryption Block). Each encryption block is constituted by an initial vector (IV (Initial Vector))the seed (Seed)and data $E_{K'c}$ (data) that enciphered contents data by key K'c.

[0046]Key K'c is constituted by the value calculated to the hash function with the application of the value Seed set to the contents key Kc by random numbers as shown in a following formula.

[0047]K'c=Hash(KcSeed)[0048]The initial vector IV and the seed Seed are set as a different value for every encryption Brock.

[0049]The data of contents is classified per 8 bytes and this encryption is performed every 8 bytes. 8 bytes of latter encryption is performed in the CBC (Cipher Block Chaining) mode performed using the result of 8 bytes of encryption of the preceding paragraph.

[0050]Since 8 bytes of encryption result of the preceding paragraph does not exist

when enciphering 8 bytes of first contents data in the case of the CBC modewhen enciphering 8 bytes of first contents dataencryption is performed by making the initial vector IV into an initial value.

[0051]By performing encryption by this CBC modeeven if one encryption Brock is decodedit is controlled that that influence attains to other encryption Brock.

[0052]About this encryptiondrawing 46 is made reference and explained in full detail behind.

[0053]About a cipher systemit does not restrict to this.

[0054]The client 1 is no charge about the contents server 3 to contents as mentioned aboveand it can acquire freely. Thereforethe contents themselves become possible [distributing] in large quantities.

[0055]Howevereach client 1 needs to hold the licensewhen using the acquired contents. Thenwith reference to drawing 6processing in case the client 1 reproduces contents is explained.

[0056]In Step S41CPU21 of the client 1 acquires the identification information (CID) of the contents to which it pointed because a user operates the input part 26. This identification information is constituted by the title of contentsthe number given for each [which is memorized] contents of everyetc.for example.

[0057]And CPU21 will read license ID (ID of a license required to use the contents) corresponding to the contentsif contents are directed. This license ID is described by the header of the contents data enciphered as shown in drawing 5.

[0058]Nextit is judged whether it progresses to Step S42and the license corresponding to license ID read at Step S41 is already acquired by the client 1and CPU21 is memorized by the storage parts store 28. When the license is not acquiredit progresses to Step S43 and CPU21 still performs license acquisition processing. The details of this license acquisition processing are later mentioned with reference to the flow chart of drawing 7.

[0059]When judged with the license already being acquired in Step S42Or in Step S43as a result of performing license acquisition processingwhen a license is acquiredit progresses to Step S44 and it is judged whether the license from which CPU21 is acquired is a thing within the term of validity. It is judged by comparing with the term (refer to drawing 8 mentioned later) specified as contents of the licenseand the present date clocked by the timer 20 whether a license is a thing within the term of validity. When judged with the term of validity of a license having already expiredit progresses to Step S45 and CPU21 performs a license update process. The details of this license update process are later mentioned with reference to the flow chart of drawing 10.

[0060]When judged with a license being still within the term of validity in Step S44Or when a license is updatedit progresses to Step S46and CPU21 reads the contents data enciphered from the storage parts store 28and is made to store it in RAM23 in Step S45. And it is the encryption block unit arranged at the data of drawing 5the

data of the encryption block memorized by RAM23 is supplied to the encryption decoding part 24and CPU21 makes it decode in Step S47 using the contents key Kc.

[0061]Although the example of the method of obtaining the contents key Kc is later mentioned with reference to drawing 15Key K_{EKBC} contained in EKB (drawing 5) can be obtained using a device node key (DNK) (drawing 8)and the contents key Kc can be obtained from data K_{EKBC} (Kc) and (drawing 5) using the key K_{EKBC}.

[0062]CPU21 supplies the contents data decoded by the encryption decoding part 24 to the codec part 25and makes it decode in Step S48 further. And from the input/output interface 32CPU21 supplies the data decoded by the codec part 25 to the outputting part 27carries out D/A conversionand makes it output from a loudspeaker.

[0063]Nextwith reference to the flow chart of drawing 7the details of the license acquisition processing performed at Step S43 of drawing 6 are explained.

[0064]The client 1 acquires the service information containing the pair of the leaves ID and DNK (Device Node Key)and the secret key and public key of the client 1the public key of a license serverand the certificate of each public key by registering with a license server a priori.

[0065]Leaf ID is a device node key required to express the identification information assigned for every clientand for DNK decode the contents key Kc which is contained in EKB (validation key blocks) corresponding to the license and which is enciphered (with reference to drawing 12it mentions later).

[0066]In Step S61CPU21 acquires first URL corresponding to license ID made into the processing object now from the header shown in drawing 5. As mentioned abovethis URL is an address which should be accessed when acquiring the license corresponding to license ID too described by the header. Thenin Step S62CPU21 accesses URL acquired at Step S61. Specificallyaccess is performed to the license server 4 by the communications department 29 via the Internet 2. At this timethe license server 4 requires the input of the license specification information that the license (license required to use contents) to purchase is specified and user IDand a passwordfrom the client 1 (Step S102 of drawing 9 mentioned later). CPU21 displays this demand on the indicator of the outputting part 27. Based on this displaya user operates the input part 26 and enters license specification informationuser IDand a password. The user of the client 1 accesses the license server 4 via the Internet 2and acquires this user ID and password a priori.

[0067]In Step S63 and S64CPU21 incorporates user ID and a password while incorporating the license identification information inputted from the input part 26. CPU21 makes the license request which controls the communications department 29 and contains the inputted user ID and leaf ID contained in license specification information and service information (it mentions later) in a password transmit to the license server 4 via the Internet 2 in Step S65.

[0068]the license server 4 is based on user IDa passwordand license specification

information so that it may mention later with reference to drawing 9 -- a license -- transmitting (Step S109) -- or a license is not transmitted when conditions are not fulfilled (Step S112).

[0069]When it judges whether the license has been transmitted from the license server 4 and the license has been transmittedit progresses to Step S67and CPU21 supplies the license to the storage parts store 28and makes it memorize in Step S66.

[0070]In Step S66when it judges with a license not being transmittedit progresses to Step S68 and CPU21 performs error handling. Since the license for using contents is not acquiredspecificallyCPU21 forbids regeneration of contents.

[0071]It becomes possible to use the contents only after acquiring the license corresponding to license ID to which each client 1 accompanies contents data as mentioned above.

[0072]License acquisition processing of drawing 7 can also be beforehand carried outbefore each user acquires contents.

[0073]The license with which the client 1 is provided contains a service condition and leaf ID ****for exampleas shown in drawing 8.

[0074]The expiration date which can use contents for a service condition based on the licenseThe download term which can download contents based on the licenseThe number of times which can copy contents based on the license (copy frequency allowed)Based on the number of times of check-outthe number of times of the maximum check-outand its licenseThe information which shows the number of times which can copy contents to a right recordable on CD-R and PD (Portable Device)the right that a license can be shifted to ownership (acquisition state)duty to take a use logetc. is included.

[0075]Nextwith reference to the flow chart of drawing 9license offer processing of the license server 4 performed corresponding to the license acquisition processing of the client 1 of drawing 7 is explained. The composition of the client 1 of drawing 2 is quoted as composition of the license server 4 also in this case.

[0076]In Step S101CPU21 of the license server 4When it stands by until it received access from the client 1and access is receivedtransmission of user IDa passwordand license specification information is required from the client 1 which has progressed and accessed Step S102. As it mentioned aboveby processing of Step S65 of drawing 7 from the client 1. When user IDa password and leaf IDand license specification information (license ID) have been transmittedCPU21 of the license server 4 performs processing which receives and incorporates this via the communications department 29.

[0077]And in Step S103CPU21 of the license server 4 accesses the fee collection server 5 from the communications department 29and requires the crediting process of the user corresponding to user ID and a password. If the demand of a crediting process is received from the license server 4 via the Internet 2the fee collection server 5The payment history of the past of the user corresponding to the user ID and

passwordetc. are investigatedWhen the credit result which permits grant of a license when it investigates whether there is any track record of the nonpayment of the remuneration of the user's license in the past and there is no such track record is transmitted and there are a track record of nonpaymentetc.the credit result of the disapproval of license granting is transmitted.

[0078]In Step S104CPU21 of the license server 4When it judges whether the credit result from the fee collection server 5 is a credit result which permits giving a license and grant of the license is permittedIt progresses to Step S105 and the license corresponding to the license specification information incorporated by processing of Step S102 is taken out out of the license memorized by the storage parts store 28. As for the license memorized by the storage parts store 28informationincluding license IDa versionthe date and time of creationthe term of validityetc.is described beforehand. In Step S106CPU21 adds leaf ID which received with the license. In Step S107CPU21 chooses the service condition matched with the license selected at Step S105. Or by processing of Step S102when a service condition is specified from a userthe service condition is added to the service condition currently prepared beforehand again if needed. CPU21 adds the selected service condition to a license.

[0079]In Step S108CPU21 signs a license with the secret key of a license serverandtherebythe license of composition as shown in drawing 8 is generated.

[0080]Nextit progresses to Step S109 and CPU21 of the license server 4 makes the license (it has the composition shown in drawing 8) transmit to the client 1 via the Internet 2 from the communications department 29.

[0081]CPU21 of the license server 4 makes the storage parts store 28 memorize the license (a service condition and leaf ID are included) which is processing of Step S109 and transmitted now in Step S110 corresponding to the user ID and the password which were incorporated by processing of Step S102. In Step S111CPU21 performs accounting. SpecificallyCPU21 requires the accounting to the user corresponding to the user ID and password of the fee collection server 5 from the communications department 29. The fee collection server 5 performs accounting to that user based on the demand of this fee collection. It can be licensedeven if that user demands grant of a license henceforth when that user does not make payment to this accounting as mentioned above.

[0082]That issince the credit result which makes grant of a license disapproval from the fee collection server 5 is transmitted in this caseit progresses to Step S112 from Step S104and CPU21 performs error handling. CPU21 of the license server 4 outputs the message of the purport that a license cannot be givento the client 1 which controlled the communications department 29 and has accessed itandspecificallyterminates processing.

[0083]In this casesince that client 1 cannot be licensed as mentioned aboveusing those contents (decode a code) can be performed.

[0084]Drawing 10 expresses the details of the license update process in Step S45 of

drawing 6. Processing of Step S131 of drawing 10 thru/or Step S135 is the fundamentally same processing as processing of Step S61 of drawing 7 thru/or Step S65. Howeverin Step S133CPU21 incorporates license ID of the license instead of the license to purchase to update. And in Step S135CPU21 transmits user ID and license ID of the license updated with a password to the license server 4.

[0085]Corresponding to transmitting processing of Step S135the license server 4 presents a service condition so that it may mention later (Step S153 of drawing 11). Thenin Step S136CPU21 of the client 1 receives presentation of the service condition from the license server 4outputs this to the outputting part 27and displays it. A user operates the input part 26chooses a predetermined service condition out of this service conditionor newly adds a predetermined service condition. CPU21 transmits the application for purchasing the service condition (conditions which update a license) selected as mentioned above to the license server 4 at Step S137. Corresponding to this applicationthe license server 4 transmits a final service condition so that it may mention later (Step S154 of drawing 11). Thenin Step S138CPU21 of the client 1 acquires the service condition from the license server 4and updates the service condition in Step S139 as a service condition of the corresponding license already memorized by the storage parts store 28.

[0086]Drawing 11 expresses the license update process which the license server 4 performs corresponding to the license update process of the above client 1.

[0087]Firstin Step S151in Step S152CPU21 of the license server 4 will receive the license specification information which the client 1 transmitted at Step S135 with license update request informationif access from the client 1 is received.

[0088]In Step S153if the update request of a license is receivedCPU21 will read the service condition (service condition to update) corresponding to the license from the storage parts store 28and will transmit to the client 1.

[0089]In [if it applies for the purchase of a service condition from the client 1 by processing of Step S137 of drawing 10 to this presentation as mentioned above] Step S154CPU21 of the license server 4 generates the data corresponding to the service condition for which it appliedand transmits to a client and 1 in Step S154. The client 1 updates the service condition of the already registered license using the service condition received by processing of Step S139as mentioned above.

[0090]In this inventionas shown in drawing 12the key of a device and a license is managed based on the principle of a broadcasting yne KURIPUSHON (Broadcast Encryption) method. A key is made into a hierarchy tree structure and leaf (leaf) of the bottom corresponds to the key of each device. In the case of the example of drawing 1216 devices from the number 0 to the number 15 or the key corresponding to a license is generated.

[0091]Each key is specified corresponding to each node of the tree structure shown by a figure Nakamaru seal. In the keys K00 thru/or K11in this examplethe key K000 thru/or the key K111 correspond [corresponding to the root node of the highest rung

/ the route key KR / the key K0 and K1] corresponding to the node of the 4th step corresponding to the 3rd step of noderespectively corresponding to the 2nd step of node. And the keys K0000 thru/or K1111 support the leaf (device node) as a node of the bottomrespectively.

[0092]Since it is considered as the layered structurethe key of the higher rank of the key K0010 and the key 0011 is set to K001and the key of the higher rank of the key K000 and the key K001 is set to K00for example. Like the followingthe key of the higher rank of the key K00 and the key K01 is set to K0and the key of the higher rank of the key K0 and the key K1 is set to KR.

[0093]The key using contents is managed by the key corresponding to each node of one path from the device node (leaf) of the bottom to the root node of the highest rung. For examplebased on the license corresponding to the node (leaf ID) of the number 3the key using contents is managed by each key of the path containing the key K0011K001K00K0and KR.

[0094]In the system of this inventionas shown in drawing 13it is a keying system constituted based on the principle of drawing 12and management of the key of a device and the key of a license is performed. In the example of drawing 138+24+32 steps of nodes are made into a tree structureand a category corresponds to each node from a root node to eight steps of a low rank. The category in here means categoriessuch as a category of the apparatus which uses semiconductor memorysuch as a memory stickfor exampleand a category of apparatus which receives digital broadcasting. And this system (T system is called) corresponds to one node in this category node as a system which manages a license.

[0095]That isa license corresponds by the key corresponding to 24 steps of a younger hierarchy's nodes further from the node of this T system. In the case of this exampletherebythe license of 2^{24} (about 16 mega) can be specified. 32 steps of lower hierarchies can prescribe the user (or client 1) of 2^{32} (about 4 giga). The key corresponding to 32 steps of nodes of the bottom constitutes DNK (Device Node Key)and ID corresponding to the leaf of the bottom is set to leaf ID.

[0096]Each device and the key of a license correspond to one of the paths which comprise each node of 64 (=8+24+32) stages. For examplethe contents key which enciphered contents is enciphered using the key corresponding to the node which constitutes the path assigned to the corresponding license. It is enciphered using the key of the hierarchy of the latest low rankand the key of the hierarchy of a higher rank is arranged in EKB (with reference to drawing 15it mentions later). DNK of the bottom is not arranged in EKBbut is described by service informationand is given to a user's client 1. the client 1 is described in EKB using the key which decoded the key of the hierarchy of the latest higher rank described in EKB (drawing 15) distributed with contents data using DNK described by the licenseand decoded and obtained it ── the key of the hierarchy on it is decoded to a pan. By performing the above processing one by onethe client 1 can obtain all the keys belonging to the path of the

license.
[0097]The concrete example of a classification of the category of a hierarchy tree structure is shown in drawing 14. In drawing 14route key KR2301 is set to the highest rung of a hierarchy tree structurethe node key 2302 is set to the following intermediate stagesand the leaf key 2303 is set to the bottom. Each device holds each leaf keyand a series of node keys from a leaf key to a route key and a route key.
[0098]The predetermined node of the Mth step (the example of drawing 13 M= 8) is set up as the category node 2304 from the highest rung. That islet each of the node of the Mth step be a device setting-out node of a specific category. Let M+1 or less step of nodeand a leaf be the node and leaf about the device contained in the category by making one node of the Mth step into the peak.
[0099]For examplea category [memory stick (trademark)] is set to the one node 2305 of the Mth step of drawing 14and the node which stands in a row below in this nodeand a leaf are set up as the node or leaf only for a category containing various devices which use memo RISUTEIIKU. That is2305 or less node is defined as the related node of the device defined as the category of a memory stickand a set of a leaf.
[0100]The low-ranking stage can be set up as the subcategory node 2306 by several steps from M stage. In the example of drawing 14the node 2306 of [the vessel only for reproduction] is set up as a subcategory node contained in the category of the device which uses a memory stick for the node under two steps of the category [memory stick] node 2305. To 2306 or less node of the vessel only for reproduction which is a subcategory node. The node 2307 of the telephone with a music reproduction function included in the category of the vessel only for playback is set upand the [PHS] node 2308 contained in the low rank at the category of a telephone with a music reproduction function and the [cellular-phone] node 2309 are set up further.
[0101]A category and a subcategory only not only in the kind of devicefor example A certain makerIt is possible to set up in arbitrary units (these are generically called an entity hereafter)such as the node which a content providera settlement-of-accounts organizationetc. manage uniquelyi.e.a batcha jurisdiction unitor a providing service unit. For exampleif one category node is set up as a peak node only for game machine machine XYZ which a game machine machine maker sellsIn the game machine machine XYZ which a maker sellsthe node key of the lower berth below the peak nodeStorebecome a leaf key possible to sell and Distribution of after that and enciphered contentOr the validation key blocks (EKB) constituted by the node key below the peak node key and the leaf key in distribution of various keys and an update process are generated and distributedand distribution of available data is attained only to the device below a peak node.
[0102]Thusby considering the following nodes as the category defined as the peak nodeor the composition set up as a related node of a subcategory by making one node into the peakThe maker which manages one peak node of the category stage or

the subcategory stagea content provideretc. generate uniquely the validation key blocks (EKB) which make the node the peakThe composition distributed to the device belonging to below a peak node is attainedand renewal of a key can be performedwithout affecting at all the device belonging to the node of other categories which do not belong to a peak node.

[0103]For examplein the tree structure shown in drawing 12the four devices 012and 3 contained in one group hold the key K00 common as a node keyK0and KR. By using this node key share compositionit becomes possible to provide only the devices 012and 3 with a common contents key. For exampleif node key K00 the very thing held in common is set up as a contents keysetting out of a contents key only with the common devices 012and 3 is possiblewithout performing new key sending. If the value Enc (K00Kcon) which enciphered the new contents key Kcon by the node key K00 is stored in a recording medium via a network and distributed to the devices 012and 3Only the devices 012and 3 become possible [solving the code Enc (K00 Kcon) using the share node key K00 held in each deviceand obtaining the contents key Kcon]. It is shown that Enc (KaKb) is the data which enciphered Kb by Ka.

[0104]When it is revealed in t at a certain time that the key K0011 which the device 3 ownsK001K00K0and KR were analyzed by the aggressor (hacker)and it was exposed of KRAfter itin order to protect the data transmitted and received by a system (group of the devices 012and 3)it is necessary to separate the device 3 from a system. for that purpose — a node key — K — 001 — K — 00 — K — zero — KR — respectively — being new — a key — K — (— t —) — 001 — K — (— t —) — 00 — — K — (— t —) — zero — K — (— t —) — R — updating — a device — zero — one — two — the — updating — a key — it is necessary to tell . Hereit is shown that K(t) aaa is an updating key of the generation (Generation) t of the key Kaaa.

[0105]distribution **** of an updating key — it ****** just. The renewal of a key the table constituted by the block data called the validation key blocks (EKB:Enabling Key Block) shown in drawing 15 Afor example via a networkOr it performs by storing in a recording medium and supplying the devices 01and 2. Validation key blocks (EKB) are constituted by the cryptographic key for distributing the key newly updated by the device corresponding to each leaf (node of the bottom) which constitutes a tree structure as shown in drawing 12. Validation key blocks (EKB) may be called renewal Brock of a key (KRB:Key Renewal Block).

[0106]The validation key blocks (EKB) shown in drawing 15 A are constituted as block data with the data configuration which can update only the required device of renewal of a node key. In the devices 01and 2 in the tree structure shown in drawing 12the example of drawing 15 A is the block data formed for the purpose of distributing the generation's t updating node key. drawing 12 — from — being clear — as — a device — zero — a device — one — updating — a node key — ****** — K — (— t —) — 00 — K — (— t —) — zero — K — (— t —) — R — required — a device — two — updating — a node key — ****** — K — (— t —) — 001 — K — (— t —) — 00 —

– K — (— t —) — zero — K — (— t —) — R — being required .

[0107]As shown in EKB of drawing 15 Atwo or more cryptographic keys are contained in EKB. The cryptographic key of the bottom of drawing 15 A is Enc (K0010K(t)001). this — a device — two — having — a leaf key — K — 0010 — enciphering — having had — updating — a node key — K — (— t —) — 001 — it is — a device — two — self — having — a leaf key — K — 0010 — this — a cryptographic key — decoding — updating — a node key — K — (— t —) — 001 — it can obtain . using updating node key K(t)001 obtained by decodingdecoding of the 2nd step of cryptographic key Enc (K — (— t —) — 001 — K — (— t —) — 00) is attained from under drawing 15 Aand updating node key K(t)00 can be obtained.

[0108]One by one below by decoding the 2nd step of cryptographic key Enc (K (t) 00K(t)0) from on drawing 15 A. Updating node key K (t) 0 is obtained and updating route key K(t) R is obtained from on drawing 15 A using this by decoding the 1st step of cryptographic key Enc (K(t) 0 and K (t) R).

[0109]on the other hand — a node key — K — 000 — updating — an object — containing — not having — a node — zero — one — updating — a node key — ****** — being required — a thing — K — (— t —) — 00 — K — (— t —) — zero — K — (— t —) — R — it is . The nodes 0 and 1 acquire updating node key K(t)00 from on drawing 15 A using the debye skiing K0000 and K0001 by decoding the 3rd step of cryptographic key Enc (K000K(t)00)belowone by oneupdating node key K(t)0 is obtained by decoding the 2nd step of cryptographic key Enc (K — (— t —) — 00 — K — (— t —) — 0) from on drawing 15 Aand updating route key K(t) R is obtained by decoding the 1st step of cryptographic key Enc (K(t) 0 and K (t) R) from on drawing 15 A. Thusthe devices 01and 2 can obtain updated key K(t) R.

[0110]The index of drawing 15 A shows the actual address of the node key and leaf key which are used as a decryption key for decoding the cryptographic key on the right-hand side of a figure.

[0111]When renewal of node key K(t) 0 and K (t) R of the upper stage of the tree structure shown in drawing 12 is unnecessary and the update process of only the node key K00 is requiredBy using the validation key blocks (EKB) of drawing 15 Bupdating node key K(t)00 can be distributed to the devices 01and 2.

[0112]EKB shown in drawing 15 B is available when distributing the new contents key sharedfor example in a specific group. As an examplethe recording medium with the devices 012and 3 in the group who shows by a dotted line is used for drawing 12and suppose that new common contents key K(t) con is required. this — the time — a device — zero — one — two — three — being common — a node key — K — 00 — having updated — K — (— t —) — 00 — using — being new — being common — updating — a contents key — K — (— t —) — con — having enciphered — data — Enc (K (t) 00K(t) con) — drawing 15 — B — being shown — having — EKB — distributing — having . By this distributionthe distribution as data of the device 4 etc. which other groups' apparatus cannot decode is attained.

[0113]That isif the devices 01and 2 decode a cryptogram using key K(t)00 which processed and obtained EKBit will become possible to obtain contents key K(t) con in t time.

[0114]As an example of processing which obtains contents key K(t) con in t time to drawing 16K (t) Processing of the device 0 which received the data Enc (K (t) 00K(t) con) which enciphered new common contents key K(t) con using 00and EKB shown in drawing 15 B via the recording medium is shown. That isthis example is an example which set the encryption message data based on EKB to contents key K(t) con.

[0115]As shown in drawing 16the device 0 generates node key K(t)00 by same EKB processing with having mentioned above using EKB at the generation t time stored in the recording mediumand the node key K000 which he stores beforehand. Using updating node key K(t)00 decodedthe device 0 decodes updating contents key K(t) conand in order to use it behindby the leaf key K0000 which he hasit enciphers and it stores it.

[0116]The example of a format of validation key blocks (EKB) is shown in drawing 17. The version 601 is an identifier which shows the version of validation key blocks (EKB). A version has the function to identify the newest EKBand a function which shows a correspondence relation with contents. A depth shows the hierarchy number of the hierarchy tree to the device of the distribution destination of validation key blocks (EKB). The data pointer 603 is a pointer in which the position of the data division 606 in validation key blocks (EKB) is shownand is a pointer which the tag pointer 604 shows the position of the tag part 607 toand the signature pointer 605 shows the position of the signature 608.

[0117]The data division 606 stores the data which enciphered the node key updatedfor example. For exampleeach cryptographic key about the updated node key as shown in drawing 16 is stored.

[0118]The tag part 607 is a tag in which the physical relationship of the node key and leaf key which were stored in the data division 606and which were enciphered is shown. The grant rule of this tag is explained using drawing 18.

[0119]Drawing 18 shows the example which sends the validation key blocks (EKB) previously explained by drawing 15 A as data. The data at this time comes to be shown in the table of drawing 18 B. Let the address of the top node contained in the cryptographic key at this time be a top node address. Since updating key K(t) R of the route key is contained in the case of this examplea top node address serves as KR. At this timethe data Enc (K(t) 0 and K (t) R) of the highest rung corresponds to the position P0 shown in the hierarchy tree shown in drawing 18 Afor example. The data of the following stage is Enc (K (t) 00K(t)0)and corresponds to the position P00 at the lower left of front data on a tree. When it sees from the position of a tree structure and data is in the bottom of it0 and when there is nothinga tag is set as 1 for a tag. A tag is set up as {a left (L) tag and a right (R) tag}. Since there is data in the position P00 at the lower left of the position P0 corresponding to the data Enc (K(t) 0 and K

(t) R) of the highest rung of drawing 18 B and there is no data in L tag =0 and the rightit is set to R tag =1. Hereaftera tag is set as all the data and the data row shown in drawing 18 C and a tag sequence are constituted.

[0120]A tag is set up in order that the corresponding data Enc (KxxxKyyy) may show where [of a tree structure] it is located. the key data Enc (KxxxKyyy) stored in the data division 606 —— although ... is only enumeration data of the key enciphered simplydistinction of the position on the tree of the cryptographic key stored as data with the tag mentioned above of it is attained. The node index to which encryption data was made to correspond is used like composition of that previous drawing 15 explainedwithout using the tag mentioned abovefor exampleit is 0:Enc (K(t) 0 and K (t) R).

00:Enc(K(t)00K(t)0

000:Enc(K((t)000K(t)00)

Although it is also possible to consider it as a data configuration like ...if it has composition using such an indexin the distribution etc. which it becomes redundant dataand data volume increasesand pass a networkit is not desirable. On the other handdistinction of a key position is attained with small data volume by using the tag mentioned above as index data in which a key position is shown.

[0121]It returns to drawing 17 and an EKB format is explained further. For examplethe signature (Signature) 608 published validation key blocks (EKB)it is an electronic signature which a lock management center (license server 4)contents ROBAIDA (contents server 3)a settlement-of-accounts organization (fee collection server 5)etc. perform. It checks that the devices which received EKB are the validation key blocks (EKB) which the just validation key-blocks (EKB) publisher published by signature verification.

[0122]When processing using the contents supplied from the contents server 3 is summarized based on the license supplied from the license server 4 as mentioned aboveit comes to be shown in drawing 19.

[0123]That iswhile contents are provided from the contents server 3 to the client 1a license is supplied to the client 1 from the license server 4. Contents are enciphered by the contents key Kc (Enc (KcContent))and the contents key KcIt is added to the contents which were enciphered by the route key KR (it is a key obtained from EKB and corresponds to key K_{EKBC} in drawing 5) (Enc (KRKc))and were enciphered with EKBand is provided for the client 1.

[0124]As shown in drawing 20the route key KR enciphered by DNK is contained in EKB in the example of drawing 19for example (Enc (DNKKR)). Thereforethe client 1 can obtain the route key KR from EKB using DNK contained in service information. The contents key Kc can be decoded from Enc (KRKc) using the route key KRand contents can be decoded from Enc (KcContent) using the contents key Kc.

[0125]Thusaccording to the principle explained with reference to drawing 12 and drawing 15RIBOKU (revoke) of each client 1 becomes possible by assigning DNK

individually to the client 1.

[0126]By adding and distributing license leaf IDin the client 1matching of service information and a license will be performed and it becomes possible to prevent the illegal copy of a license.

[0127]It also enables an end user to create the contents which can prevent an illegal copy by distributing the certificate and secret key for clients as service information using these.

[0128]Use of a certificate and a secret key is later mentioned with reference to the flow chart of drawing 28.

[0129]In this inventionsince T system which manages a licenseand the category using various kinds of contents of a device are matched with a category node as explained with reference to drawing 13two or more DNK(s) can be given to the same device. As a resultit becomes possible to manage the contents of a different category with one device.

[0130]Drawing 21 expresses this relation. That isbased on T systemthe license using the contents 1 to which DNK1 is assigned is recorded on the device D1. Similarlythe contents 2 to which DNK2 was assigned and which carried out ripping to the memory stick from CD are recordable on this device D1for example. In this casethe device D1 becomes possible [treating simultaneously contents which are called the contents 1 and the contents 2 and which were distributed by a different system (T system and a device management system)]. Such a thing cannot be performedwhen assigning new DNKand DNK already assigned is deleted and it is made to make only one DNK correspond to a device.

[0131]By assigning the license category 1 and the license category 2 which are shown in drawing 22 at each of three square shapes each of 32 lower hierarchies[in / drawing 13] It becomes possible to classify the inside of the same category into small meetingssuch as a genre of contentsa labela storeand distribution serviceand to manage it using a subcategory.

[0132]In the example of drawing 22the license category 1 belongs to the genre of jazzand the license category 2 belongs to the genre of a lockfor example. License ID makes the contents 1 and the contents 2 which are 1 correspond to the license category 1and the user 1 thru/or the user 3 are supplied widelyrespectively. The contents 3 of license ID2the contents 4and the contents 5 are containedand the user 1 and the user 3 are provided with the license category 2respectively.

[0133]Thusin this inventionthe key management which became independent for every category becomes possible.

[0134]DNK is beforehand embedded to neither apparatus nor mediabut by the license server 4when performing registration processingthe system which can purchase the key by a user can be realized by making it download to each apparatus or media.

[0135]After it is created contentseven if what kind of usage is carried outit is concerned with the usagethere areand it is desirable in all the uses that it is usable.

[no] For examplealso in a different contents distribution service or the domain in which service conditions differit is desirable that the same contents can be used. In this inventionfor this reasonas mentioned abovethe certificate (certificates) of a secret key and the public key corresponding to it is distributed to each user (client 1) from the license server 4 as a certificate authority. Using the secret keyeach user can create a signature (signature)can add to contentsand can guarantee genuine [of contents] (integrity)and can aim at prevention from an alteration of contents.

[0136]The example of processing in this case is explained with reference to the flow chart of drawing 23. Processing of drawing 23 explains the ripping processing a user makes the storage parts store 28 remember the data played from CD to be.

[0137]Firstin Step S171CPU21 of the client 1 incorporates the regenerative data of CD inputted via the communications department 29 as record data. In Step S172CPU21 judges whether the watermark is contained in the record data incorporated by processing of Step S171. This watermark is constituted by the copy management information (CCI) of a tripletand the 1-bit trigger (Trigger)and is embedded in the data of contents. It progresses to Step S173 and CPU21 performs processing which extracts the watermarkwhen a watermark is detected. When a watermark does not existprocessing of Step S173 is skipped.

[0138]Nextin Step S174CPU21 creates the data of the header recorded corresponding to contents. The data of this header is constituted by URL showing the access point for acquiring content IDlicense IDand a licenseand the watermark.

[0139]Nextit progresses to Step S175 and CPU21 creates the digital signature based on the data of the header created by processing of Step S174 using its own secret key. This secret key is acquired from the license server 4 (Step S67 of drawing 7).

[0140]CPU21 controls the encryption decoding part 24 by Step S176and contents are made to encipher by a contents key. A contents key is simultaneously acquiredwhen contents are acquired (drawing 5 or drawing 19).

[0141]Nextfor exampleCPU21 makes data record on the magneto-optical disc 43 constituted with a mini disc etc. in Step S177 based on a file format.

[0142]When a recording medium is a mini discCPU21 supplies contents to the codec part 25for examplemakes contents code with ATRAC3 method in Step S176. And the coded data is further enciphered by the encryption decoding part 24.

[0143]Drawing 24 expresses typically the state where contents were recorded on the recording medium as mentioned above. The watermark (WM) extracted from the contents (E (At3)) enciphered is recorded out of contents (header).

[0144]Drawing 25 expresses the more detailed composition of the file format in the case of recording contents on a recording medium. In this examplecontent ID (CID)license ID (LID)URL and the header containing a watermark (WM) are recordedand also. EKBthe data (Enc (KRKc)) which enciphered the contents key Kc by the route key KRA certificate (Cert)the digital signature (Sig (Header)) generated based on the headerthe data (Enc (KcContent)) which enciphered contents by the

contents key Kcthe metadata (Meta Data)and the mark (Mark) are recorded.

[0145]Although the watermark is embedded to the inside of contentsAs shown in drawing 24 and drawing 25the inside of contents is making it arrange in a header independentlyand it becomes possible to detect the information currently embedded to contents as a watermark promptly and simply. Thereforeit can be judged promptly whether the contents can be copied.

[0146]Metadata expresses the data of a jacketa photographwordsetc.for example. A mark is later mentioned with reference to drawing 31.

[0147]Drawing 26 expresses the example of the public key certification as a certificate. A public key certification is usually a certificate which the certificate authority (CA:Certificate Authority) in a public-key crypto system publishesA certificate authority adds informationincluding the term of validity etc.to self IDpublic keyetc. which the user submitted to the certificate authorityadds the digital signature by a certificate authority further to themand is created. In this inventionsince the license server 4 (or contents server 3) also publishes a certificatea secret keytherefore a public keythe user can get this public key certification by providing the license server 4 with user IDa passwordetc.and performing registration processing.

[0148]The consecutive numbers of the certificate in which the version number of a certificate and the license server 4 assign the public key certification in drawing 26 to the user (user) of a certificateThe algorithm used for the digital signature and a parameterthe name of a certificate authority (license server 4)the term of validity of a certificatea certificate user's ID (node ID or leaf ID)and the certificate user's public key are contained as a message. The digital signature created by the license server 4 as a certificate authority is added to this message. This digital signature is the data generated using the secret key of the license server 4 based on the hash value generated with the application of the hash function to the message.

[0149]in the case of the example of drawing 12if node ID or leaf ID is the device 0it will be set to "0000"if it comes out device 1it will be set to "0001"and if it is the device 15it will be set to "1111"for example. Based on such IDit is identified whether the device (entity) is an entity located in which position (a leaf or node) of tree composition.

[0150]Thusdistribution of contents will be freely performed by dissociating and distributing a license required to use contents with contents. The contents which came to hand in arbitrary methods or a course can be dealt with unitary.

[0151]By what a file format is constituted for as shown in drawing 25. When distributing the contents of the format via the Internetwhen it provides for SDMI (Secure Digital Music Initiative) apparatusof courseit becomes possible to manage the copyright of contents.

[0152]As shown in drawing 27 for exampleeven if contents are provided via a recording mediumEven if provided via the Internet 2the same processing enables it to check out to predetermined PD (Portable Device) as SDMI (Secure Digital Music

Initiative) apparatusetc.

[0153]Nextwith reference to the flow chart of drawing 28processing in case the client 1 checks out contents to other clients (for examplePD) is explained.

[0154]Firstin Step S191CPU21 judges whether the digital signature is added to contents. When judged with the digital signature being addedit progresses to Step S192and CPU21 extracts a certificate and performs processing verified by the public key of a certificate authority (license server 4). That isthe client 1 acquires the public key corresponding to the secret key of the license server 4 to the license server 4and decodes the digital signature added to the public key certification by the public key. As explained with reference to drawing 26the digital signature is generated based on the secret key of a certificate authority (license server 4)and can be decoded using the public key of the license server 4. CPU21 calculates a hash value with the application of a hash function to the whole message of a certificate. And if CPU21 compares the calculated hash value with the hash value produced by decoding a digital signature and both are in agreementit will judge with a message not being what was altered. When both are not in agreementit will be said that this certificate is altered.

[0155]Thenin Step S193CPU21 judges whether the certificate is altered or notand when judged with not being alteredit progresses to Step S194 and it performs processing which verifies a certificate by EKB. This verification processing is performed by investigating whether EKB can be followed or not based on leaf ID (drawing 26) contained in a certificate. This verification is explained with reference to drawing 29 and drawing 30.

[0156]Nowas shown in drawing 29suppose that it is the device [RIBOKU / device / the device which has the leaf key K1001]. At this timedata (cryptographic key) as shown in drawing 30and EKB which has a tag are distributed to each device (leaf). This EKB is EKB which updates the key KRK1K10and K100in order RIBOKU [the device "1001" in drawing 29].

[0157]All the leaves other than a RIBOKU device "1001" can acquire updated route key K(t) R. That issince the leaf which stands in a row in the low rank of the node key K0 holds in a device the node key K0 which is not updatedit can acquire updating route key K(t) R by decoding the cryptographic key Enc (K0K(t) R) by the key K0.

[0158]The leaf not more than node key K11 can acquire updating node key K(t)1 using the node key K11 which is not updated by decoding Enc (K11K(t)1) by the node key K11. It becomes possible by decoding Enc (K(t) 1 and K (t) R) by node key K(t)1 to acquire updating route key K(t) R. Also about the low rank leaf of the node key K101it is possible to acquire updating route key K(t) R similarly.

[0159]The device "1000" which has the leaf key [RIBOKU / leaf key] K1000Enc (K1000K(t)100) is decoded by the self leaf key K1000node key K(t)100 can be acquiredthe node key of a higher rank can be further decoded one by one using thisand updating route key K(t) R can be acquired.

[0160]on the other hand -- RIBOKU -- having had -- a device -- "1001" -- self -- a leaf -- one -- a step -- a top -- updating -- a node key -- K -- (-- t --) -- 100 -- EKB -- processing -- being unacquirable -- since -- after all -- updating -- a route -- a key -- K -- (-- t --) -- R -- being unacquirable .

[0161]The data shown in drawing 30 and EKB which has a tag are distributed and stored in the just device [RIBOKU / device] (client 1) from the license server 4.

[0162]Theneach client can perform EKB tracking processing using the tag. This EKB tracking processing is processing which judges whether a key distribution tree can be followed from the route key of a higher rank.

[0163]For example1001which is ID (leaf ID) of the leaf "1001" of drawing 29 is grasped as 4 bits of "1"00and "1"and it is judged one by one from the most significant bit whether a tree can be followed according to a lower bit. In this judgmentif a bit is 1it will go to right-hand sideand if it is 0processing which goes to left-hand side will be performed.

[0164]Since the most significant bit of ID "1001" is 1it goes to right-hand side from the route key KR of drawing 29. It is judged with the tag (tag of the number 0) of the beginning of EKB being 0: {00}and being what has data on both branches. In this casesince it can go to right-hand sideit can arrive at the node key K1.

[0165]Nextit progresses to the node of the low rank of the node key K1. Since the 2nd bit of ID "1001" is 0it goes to left-hand side. The tag in which the tag of the number 1 expresses the existence of the data of the low rank of the left-hand side node key K0and the existence of the data of the low rank of the node key K1 is shown is a tag of the number 2. As shown in drawing 30this tag shall be 2: {00}and shall have data on both branches. Thereforeit can go to left-hand side and can arrive at the node key K10.

[0166]The 3rd bit of ID "1001" is 0 and goes to left-hand side. At this timethe tag (tag of the number 3) in which the existence of the data of the low rank of K10 is shown is 3: {00}and it judges that it has data on both branches. Thenit can go to left-hand side and can arrive at the node key K100.

[0167]The least significant bit of ID "1001" is 1and goes to right-hand side. The tag which the tag of the number 4 corresponds to the node key K11and expresses the numerals of the data of the low rank of K100 is a tag of the number 5. This tag is 5: {01}. Thereforedata will not exist in right-hand side. as a resultarrive at a node "1001" -- it is judged with there being nothing and the device of ID "1001" being the device which cannot acquire the updating route key by EKBi.e.a RIBOKU device.

[0168]On the other handfor examplethe device ID which has the leaf key K1000 is "1000"and like the case where it mentions aboveif EKB tracking processing based on the tag in EKB is performedit can arrive at a node "1000." Thereforeit is judged with the device of ID "I000" being a just device.

[0169]Return to drawing 28 and CPU21 based on the verification processing of Step S194When RIBOKU [***** / RIBOKU / the certificate / is judged at Step S195 and

/ the certificate]it progresses to Step S196 and processing which verifies a digital signature by the public key contained in a certificate is performed.

[0170]That isas shown in <u>drawing 26</u>the certificate user's (contents creator) public key is contained in the certificateand the signature (Sig (Header)) shown in <u>drawing 25</u> is verified using this public key. By namelythe thing for which the data (hash value) produced by decoding the digital signature Sig (Header) is compared with the hash value calculated with the application of the hash function to Header shown in <u>drawing 25</u> using this public key. It can check that Header is not alteredif both are in agreement. On the other handit will be said that Header is altered if both are not in agreement.

[0171]In Step S197CPU21 judges whether Header is altered or notand if not alteredit progresses to Step S198 and it verifies a watermark. In Step S199CPU21 judges whether he can check out or not as a result of verification of a watermark. When you can check outit progresses to Step S200 and CPU21 performs check-out. That iscontents are made to transmit and copy to the client 1 of a check-out place.

[0172]In [when judged with a digital signature not existing in Step S191] Step S193In [when judged with the certificate being altered] Step S195When are judged with the ability of a certificate to have not been verified by EKB and it is judged with the header being altered in Step S197 as a result of verification of a digital signatureOr in Step S199when judged with prohibition of check-out being described by the watermarkit progresses to Step S201 and error handling is performed. That ischeck-out is forbidden in this case.

[0173]Thusit becomes possible by distributing a certificate and a secret key to a user from the license server 4and adding a digital signature at the time of contents creation to guarantee Shinsei of the maker of contents. Therebycirculation of inaccurate contents can be controlled.

[0174]A watermark is detected at the time of contents creationby giving the information to a digital signaturethe alteration of watermark information can be prevented and Shinsei of contents can be guaranteed.

[0175]As a resulteven if the contents created once are distributed with what kind of gestaltit becomes possible to guarantee Shinsei of the original contents.

[0176]Since contents do not have a service condition but the service condition is added to the licenseit is changing the service condition within a licenseand it becomes possible to change the service conditions of the contents related to it all at once.

[0177]Nextthe utilizing method of a mark is explained. In this inventionas mentioned abovea service condition is added to the license instead of contents. Howeveran operating condition may change with contents. Thenin this inventionas shown in <u>drawing 25</u>a mark is added to contents.

[0178]Since a license and contents have one-pair Oshi's relationit becomes difficult to describe each operating condition of contents only in the service condition of a

license. Thenthough management with a license is carried out by adding an operating condition to contents in this wayit becomes possible to manage each contents.

[0179]As shown in drawing 31a user's ID (leaf ID)an ownership flagbeginning-of-using timecopy frequencyetc. are described by this markfor example.

[0180]The digital signature generated based on messagessuch as leaf IDan ownership flagbeginning-of-using timeand copy frequencyis added to a mark.

[0181]An ownership flag is added when the license for which only a predetermined period makes contents usable is bought as it was for example (when duration of service is changed eternally). Beginning-of-using time is described when use of contents is started within a predetermined period. For examplewhen the stage to download contents is restricted and download is performed within the termthe time which downloaded contents actually is described here. Therebyit is proved that it is effective use within a period.

[0182]The number of times which copied the contents by then is described as a history (log) by copy frequency.

[0183]Nextwhen a user buys a license with reference to the flow chart of drawing 32a mark is explained as an example added to contents about the processing which adds a mark.

[0184]Firstin Step S221CPU21 accesses the license server 4 via the Internet 2 based on instructions of the user from the input part 26.

[0185]In Step S222CPU21 incorporates the input through the input part 26 from a userand requires acquisition of a license from the license server 4 corresponding to the input.

[0186]Corresponding to this demandthe license server 4 presents a remuneration required in order to buy a license so that it may mention later with reference to the flow chart of drawing 33 (Step S242 of drawing 33). Thenin Step S223this will be outputted to the outputting part 27 and CPU21 of the client 1 will display itif presentation of the remuneration from the license server 4 is received.

[0187]A user judges whether based on this displayit consents to the shown remunerationand inputs that decision result from the input part 26 based on that decision result.

[0188]When it judges with CPU21 having judged whether it consented to the remuneration shown the user in Step S224 based on the input from the input part 26and having consentedit progresses to Step S225 and processing which notifies consent to the license server 4 is performed.

[0189]If this notice of consent is receivedthe license server 4 will transmit the information showing acquisition of a remunerationi.e.the mark which described the ownership flag(Step S244 of drawing 33). Thenin Step S226CPU21 of the client 1 will perform processing which embeds the received mark to contents in Step S227if the mark from the license server 4 is received. That isthe mark the ownership flag as shown in drawing 31 was described to be as a mark of the contents corresponding to

the bought license by this will be recorded corresponding to contents. Since it means that the message was updated at this timeCPU21 also updates a digital signature (drawing 25) and is recorded on a recording medium.

[0190]In Step S224when judged with not consenting to the remuneration shown from the license server 4it progresses to Step S228 and CPU21 notifies the license server 4 that it does not consent to the shown remuneration.

[0191]Corresponding to processing of such a client 1the license server 4 performs processing shown in the flow chart of drawing 33.

[0192]Namelyin Step S241first CPU21 of the license server 4If the demand of license acquisition is transmitted from the client 1 (Step S222 of drawing 32)this will be receiveda remuneration required for the acquisition by the target license will be read from the storage parts store 28 in Step S242and this will be transmitted to the client 1.

[0193]As mentioned abovethe notice of whether to consent to the remuneration shown from the client 1 to the remuneration shown by doing in this way is transmitted.

[0194]Thenin Step S243 CPU21 of the license server 4When it judges whether the notice of consent was received from the client 1 and judges with having received the notice of consentprogress to Step S244generate the mark containing the message showing the acquisition by the target licenseand with its own secret key. A digital signature is added and it transmits to the client 1. Thusthe transmitted mark is recorded on corresponding contents in the storage parts store 28 of the client 1as mentioned above (Step S227 of drawing 32).

[0195]In Step S243when judged with the notice of consent not being received from the client 1processing of Step S244 is skipped. That isin this casesince it means that acquisition processing of the license was not performed eventuallya mark is not transmitted.

[0196]Drawing 34 expresses the example of composition of the mark transmitted from the license server 4 to the client 1 in Step S244. The mark is constituted in this example by digital signature Sig_s (LeafIDOwn) generated based on the secret key S of the license server 4 in leaf IDthe ownership flag (Own)and that user's leaf ID and ownership flag.

[0197]Since this mark is effective only to a specific user's specific contentswhen copied in the target contentsthe mark which accompanies those copied contents is repealed.

[0198]Thuscontents and a license are separated and it becomes possible to realize service according to the operating condition of each contents also in the case where a service condition is made equivalent to a license.

[0199]Nexta grouping is explained. It is called a grouping to collect two or more apparatus and media suitablyand to enable it to deliver and receive contents freely in the one set. Usuallythis grouping is performed in apparatus and the media which an individual owns. Although this grouping set up the group key for every group and was

performed conventionallyit becomes possible to carry out a grouping easily by matching the same license with two or more apparatus and media which carry out grouping.

[0200]It is also possible to carry out the grouping of each apparatus by registering beforehand. The grouping in this case is explained below.

[0201]In this casethe user needs to register into a server beforehand the certificate of the apparatus made into a grouping object. The registration processing of this certificate is explained with reference to the flow chart of drawing 35 and drawing 36.

[0202]Firstwith reference to the flow chart of drawing 35the registration processing of the certificate of a client (apparatus used as a grouping object) is explained. In Step S261CPU21 of the client 1 draws up its own [as apparatus made into the object of a grouping] certificate. Its own public key is contained in this certificate.

[0203]Nextit progresses to Step S262and based on the input from a user's input part 26CPU21 accesses the contents server 3 and performs processing which transmits the certificate drawn up by processing of Step S261 to the contents server 3 in Step S263.

[0204]As a certificatewhat received from the license server 4 can also be used as it is.

[0205]All the apparatus made into a grouping object performs the above processing.

[0206]Nextwith reference to the flow chart of drawing 36the registration processing of the certificate of the contents server 3 performed corresponding to the registration processing of the certificate of the client 1 of drawing 35 is explained.

[0207]Firstin Step S271in Step S272CPU21 of the contents server 3 will register the certificate into the storage parts store 28if the certificate transmitted from the client 1 is received.

[0208]The above processing is performed for every apparatus made into a group object. As a resultas shown in drawing 37the certificate of the device which constitutes the group is registered into the storage parts store 28 of the contents server 3 for every groupfor example.

[0209]In the example shown in drawing 37the certificates C11 thru/or C14 are registered as the group's 1 certificate. Corresponding public key K_{P11} thru/or K_{P14} is contained in these certificates C11 thru/or C14.

[0210]Similarlyas the group's 2 certificatethe certificates C21 thru/or C23 are registeredand public key K_{P21} thru/or K_{P23} to which these correspond is contained.

[0211]If offer of contents is required of the apparatus which belongs to the group from a user in the state which constitutes the above groups where the certificate was registered for every apparatusthe contents server 3 will perform processing shown in the flow chart of drawing 38.

[0212]Firstin Step S281CPU21 of the contents server 3 performs processing which verifies the certificate which belongs to the group among the certificates memorized by the storage parts store 28.

[0213]This verification processing is performed by following EKB using a tag based on leaf ID contained in the certificate of each apparatusas explained with reference to drawing 29 and drawing 30. EKB is distributed also to the contents server 3 from the license server 4. The certificate [RIBOKU / certificate / this verification processing] is excepted.

[0214]In Step S282CPU21 of the contents server 3 chooses the validated certificate as a result of the verification processing of Step S281. And in Step S283CPU21 enciphers a contents key by each public key of the certificate of each apparatus selected by processing of Step S282. In Step S284CPU21 transmits with contents the contents key enciphered by processing of Step S283 to each apparatus of the target group.

[0215]Supposing RIBOKU [the certificate C14] among the groups 1 by whom it is shown to drawing 37it will be processing of Step S283 and encryption data as shown in drawing 39 will be generatedfor example.

[0216]That isthe contents key Kc is enciphered by public key K_{P11} of the certificate C11public key K_{P12} of the certificate C12or public key K_{P13} of the certificate C13 in the example of drawing 39.

[0217]Corresponding to processing as shown in drawing 38 of the contents server 3the apparatus (client) of each group who receives offer of contents performs processing shown in the flow chart of drawing 40.

[0218]Firstin Step S291CPU21 of the client 1 receives the contents which the contents server 3 has transmitted by processing of Step S284 of drawing 38 with a contents key. Contents are enciphered by the contents key Kcand the contents key is enciphered by the public key which each apparatus holds as mentioned above (drawing 39).

[0219]Thenin Step S292CPU21 decodes and acquires the contents key addressed to it with its own secret key. [who received by processing of Step S291] And decoding processing of contents is performed using the acquired contents key.

[0220]For exampleusing its own [corresponding to public key K_{P11}] secret keythe apparatus corresponding to the certificate C11 shown in the example of drawing 39 decodes the code of the contents key Kcand acquires the contents key Kc. And contents are further decoded using the contents key Kc.

[0221]Same processing is performed also in the certificate C12 and the apparatus corresponding to C13. Since the contents key Kc enciphered using its own public key is not sent along with contentsthe apparatus of the certificate [RIBOKU / certificate] C14 cannot decode the contents key Kctherefore cannot decode contents using the contents key Kc.

[0222]Although it was made to perform a grouping above to the contents key (namelycontents)it is also possible to perform a grouping to a license key (license).

[0223]Grouping becomes possiblewithout using a special group key and ICV (Integrity CheckValue) mentioned later as mentioned above. This grouping is fit for applying to a

small-scale group.
[0224]In this inventiona license is also made possible [checking outchecking in carrying out a moveor copying]. Howeverthese processings are performed based on the rule defined by SDMI.
[0225]Nextwith reference to the flow chart of drawing 41 and drawing 42check-out processing of the license by such a client is explained.
[0226]Firstprocessing of the client which checks out a license to other clients with reference to the flow chart of drawing 41 is explained. Firstin Step S301CPU21 of the client 1 reads the number of times N1 of check-out of the license for check-out. Since this number of times of check-out is written in the service condition shown in drawing 8it is read in this service condition.
[0227]Nextin Step S302CPU21 reads too the number of times N2 of the maximum check-out of the license for check-out in the service condition of a license.
[0228]And in Step S303 CPU21The number of times N1 of check-out read by processing of Step S301 is compared with the number of times N2 of the maximum check-out read by processing of Step S302and it is judged whether the number of times N1 of check-out is larger than the number of times N2 of the maximum check-out.
[0229]When it judges that the number of times N1 of check-out is smaller than the number of times N2 of the maximum check-outprogress to Step S304 and CPU21The leaf key of the device (client of a check-out place) of the other party is acquired from the device of partner eachand the leaf key is stored in the check-out list of storage parts stores 28 corresponding to license ID made applicable to check-out now.
[0230]Nextin Step S305only 1 *************s the value of the number of times N1 of check-out of the license in which CPU21 was read by processing of Step S301. In Step S306CPU21 calculates ICV based on the message of a license. This ICV is later mentioned with reference to drawing 46 thru/or drawing 50. It becomes possible to prevent the alteration of a license using ICV.
[0231]NextCPU21 enciphers using its own public keyand makes ICV calculated by the license for check-outand processing of Step S306 output and copy to the device of the other party with EKB and a certificate in Step S307. CPU21 makes ICV calculated by processing of Step S306 remember it to be a leaf key of an opposite party device in the check list of the storage parts store 28 in Step S308 corresponding to license ID.
[0232]In Step S303when judged with the number of times N1 of check-out not being smaller than the number of times N2 of the maximum check-out (for exampleequal)since check-out is performedonly the number of times already permitted cannot check out any more. Thenit progresses to Step S309 and CPU21 performs error handling. That ischeck-out processing will be performed in this case.
[0233]Nextwith reference to the flow chart of drawing 42check-out processing of drawing 41 explains processing of the client which receives check-out of a license.

[0234]Firstin Step S321its own leaf key is transmitted to an opposite party device (client 1 which checks out a license). This leaf key is memorized by the client of the other party in Step S304 corresponding to license ID.

[0235]Nextin Step S322CPU21 receives thiswhen the license and ICV which were enciphered from the client 1 of the other party have been transmitted with EKB and a certificate. That isthis licenseICVEKBand a certificate are transmitted from the device of the other party by processing of Step S307 of drawing 41.

[0236]CPU21 makes the storage parts store 28 memorize the license received by processing of Step S322ICVEKBand a certificate in Step S323.

[0237]The client 1 which received check-out of the license as mentioned above performs processing shown in the flow chart of drawing 43when using the license which received check-out and reproducing predetermined contents.

[0238]That isin Step S341CPU21 of the client 1 calculates first ICV of the contents as which reproduction was specified by the user via the input part 26. And CPU21 makes ICV which is memorized by the storage parts store 28 and which is enciphered decode in Step S342 based on the public key contained in the certificate.

[0239]Nextin Step S343it is judged whether ICV calculated now by processing of Step S341 and ICV of CPU21 which was read by processing of Step S342 and decoded correspond. The license will be altered when both are in agreement. Thenit progresses to Step S344 and CPU21 performs processing which reproduces corresponding contents.

[0240]On the other handin Step S343when judged with two ICV(s) not being in agreementa license has a possibility that it may be altered. For this reasonit progresses to Step S345 and CPU21 performs error handling. That isat this timecontents can be reproduced using that license.

[0241]Nextprocessing of the client which receives check-in of the license once checked out to other clients as mentioned above is explained with reference to the flow chart of drawing 44.

[0242]Firstin Step S361CPU21 acquires the leaf key of the device (client 1 which returns a license (check-in)) of the other partyand ID of the license for check-in. Nextin Step S362CPU21 judges whether the license for [which was acquired at Step S361] check-in is a license which he checked out to the opposite party device. This judgment is performed based on ICV memorized by processing of Step S308 of drawing 41a leaf keyand license ID. That iswhen it is judged and memorized whether the leaf key acquired at Step S361 and the licenses ID and ICV are memorized during the check-out listit is judged with it being the license which he checked out.

[0243]In Step S363a license requires deletion of the license of the device of the other partyEKBand a certificate CPU21when he checks out. Based on this demandthe device of the other party performs deletion of a licenseEKBand a certificate so that it may mention later (Step S383 of drawing 45).

[0244]In Step S364since the once checked-out license has checked in at CPU21

againonly 1 carries out the decrement of the number of times N1 of check-out of the license.

[0245]In Step S365it is judged whether CPU21 has checked out other licenses to the device of the other partyWhen other licenses which he has still checked out do not existit progresses to Step S366 and CPU21 deletes the memory in the check-out list as check-in subject equipment of the device of the other party. On the other handin Step S365since check-in of other licenses may be received when judged with other licenses which he has checked out to the device of the other party existingprocessing of Step S366 is skipped.

[0246]In Step S362when it judges that the license made applicable to check-in is not a license which he checked out to the opposite party deviceit progresses to Step S367 and CPU21 performs error handling. That isin this casesince it will not be the license which he has jurisdiction overcheck-in processing is not performed.

[0247]when a user copies a license unjustlythe value of ICV memorized differs from the value of ICV calculated based on the license acquired by processing of Step S361 ーー he can come out and check in.

[0248]Drawing 45 expresses processing of the client made to check in at the license which he has to the client which performs check-in processing of the license shown in the flow chart of drawing 44.

[0249]In Step S381CPU21 of the client 1 transmits ID of the license a leaf key and for check-in to the device (client 1 which performs processing shown in the flow chart of drawing 44) of the other party. As mentioned abovein Step S361the device of the other party acquires this leaf key and license IDand performs authenticating processing of the license for check-in in Step S362 based on it.

[0250]In Step S382CPU21 of the client 1 judges whether deletion of the license was required from the device of the other party. Namelywhen a license is a license for [just] check-inas mentioned aboveas for the device of the other partydeletion of a licenseEKBand a certificate is required by processing of Step S363. Thenwhen this demand is receivedit progresses to Step S383 and CPU21 deletes a licenseEKBand a certificate. That issince this client 1 will be in the state where that license cannot be used henceforth and DEKURI mend of the number of times N1 of check-out is carried out only for 1 by processing of Step S364 of drawing 44it means that check-in was completed by this.

[0251]In Step S382when judged with deletion of a license not being demanded from the device of the other partyit progresses to Step S384 and error handling is performed. That ischeck-in will not be possible for the Reasons of the values of ICV differing in this case.

[0252]Although check-in and check-out were explained aboveit is possible similarly in a license a copy or for it to be made to carry out a move.

[0253]Nextin order to prevent the alteration of a license (contents are also the same)the integrity check value (ICV) of a license is generatedand it matches with a

licenseand calculation of ICV explains the processing constitution which judges the existence of a license alteration.

[0254]The integrity check value (ICV) of a license is calculatedfor example using the hash function to a licenseand is calculated by ICV=hash (KicvL1L2...). Kicv is an ICV generation key. L1 and L2 are the information on a licenseand the message authenticator (MAC:Message authentication Code) of the critical information of a license is used.

[0255]The example of MAC value generation using DES cipher-processing composition is shown in drawing 46. (dividing the target message per 8 bytesas shown in the composition of drawing 46 -- the divided message is hereafter set to) M1M2...MN -- exclusive OR of initial value (IV) and M1 is first carried out by operation part 24-1A (the result is set to I1). NextI1 is put into DES encryption section 24-1Band it enciphers using a key (hereafter referred to as K1) (an output is set to E1). Continuouslyexclusive OR of E1 and M2 is carried out by operation part 24-2Athe output I2 is put in to DES encryption section 24-2Band it enciphers using the key K1 (output E2). Hereafterthis is repeated and encryption processing is performed to all the messages. EN which came out at the last serves as a message authenticator (MAC (Message Authentication Code)) from DES encryption section 24-NB.

[0256]The integrity check value (ICV) of a license is generated by the MAC value and ICV generation key of such a license with the application of a hash function. For exampleif it will be guaranteed that there is no alteration in a license if ICV generated to the license generate time is compared with ICV newly generated based on the license and the same ICV is obtainedand ICV(s) differit will be judged with there having been an alteration.

[0257]Nextthe composition which sends Kicv which is an integrity check value (ICV) generation key of a license by above-mentioned validation key blocks is explained. That isit is the example used as the integrity check value (ICV) generation key of a license of the encryption message data based on EKB.

[0258]When a license common to two or more devices is sent to drawing 47 and drawing 48the example of composition which distributes the integrity check value generation key Kicv for verifying the existence of an alteration of those licenses by validation key blocks (EKB) is shown. Drawing 47 shows the example which distributes the check value generation key Kicv which can be decoded to the devices 012and 3and drawing 48 shows the example which carries out RIBOKU (exclusion) of the devices 01and 2 and the device 3 in threeand distributes the check value generation key Kicv which can be decoded only to the devices 01and 2.

[0259]In the example of drawing 47by updating node key K(t)00 with the data Enc (K (t) 00Kicv) which enciphered the check value generation key Kicv. a device -- zero -- one -- two -- three -- setting -- each -- having -- a node key -- a leaf key -- using -- updating -- having had -- a node key -- K -- (-- t --) -- 00 -- decoding --

being possible — validation — key blocks (EKB) — generating — distributing . As shown in the right-hand side of drawing 47first each device by processing EKB (decoding)updating — having had — a node key — K — (— t —) — 00 — acquiring — next — having acquired — a node key — K — (— t —) — 00 — using — enciphering — having had — a check — a value — generation — a key — Enc (K (t) 00Kicv) — decoding — a check — a value — generation — a key — Kicv — obtaining — things — being possible — becoming .

[0260]the other devices 456and 7 … by the node key and leaf key which self holds even if it receives the same validation key blocks (EKB). Since node key K(t)00 which processed EKB and were updated are unacquirablea check value generation key can be safely sent only to a just device.

[0261]On the other handthe example of drawing 48 noting that RIBOKU (exclusion) of the device 3 is carried out by disclosure of the key in the group enclosed with the dotted-line frame of drawing 12for examplelt is other groups' Membai.e.the example which only received without the devices 01and 2and generated and distributed the validation key blocks (EKB) which can be decoded. The data Enc (K (t) 00Kicv) which enciphered the check value generation key (Kicv) as the validation key blocks (EKB) shown in drawing 48 by the node key (K (t) 00) is distributed.

[0262]The decoding procedure is shown in the right-hand side of drawing 48. The devices 01and 2 acquire an updating node key (K (t) 00) from the received validation key blocks first by the decoding processing using the leaf key or node key which self holds. Nextthe check value generation key Kicv is acquired by decoding by K(t)00.

[0263]the devices 45and 6 of other groups who show drawing 12 — even if … receives this same data (EKB)it cannot acquire an updating node key (K (t) 00) using the leaf key and node key which self holds. Also in the device [RIBOKU / device / similarly] 3by the leaf key and node key which self holdsan updating node key (K (t) 00) cannot be acquiredbut only the device which has a just right becomes possible [decoding and using a check value generation key].

[0264]Thusif delivery of the check value generation key using EKB is useddata volume will be lessened and only a just right holder will become possible [distributing the check value generation key whose decoding was enabled] safely.

[0265]The illegal copy of EKB and an encryption license can be eliminated by using the integrity check value (ICV) of such a license. For exampleas shown in drawing 49 Athere are the media 1 which stored the license L1 and the license L2 with the validation key blocks (EKB) which can acquire each license keyand the case where this is copied to the media 2 as it was is assumed. The copy of EKB and an encryption license will be possible and this can be used with the device which can decode EKB.

[0266]In the example shown in drawing 49 Bit has composition which matches with the license justly stored in each mediaand stores an integrity check value (ICV (L1L2)). (ICV (L1L2)) shows ICV=hash (KicvL1L2) which is an integrity check value of

the license calculated by using a hash function for the license L1 and the license L2. In the composition of <u>drawing 49 B</u>the license 1 and the license 2 are justly stored in the media 1and the integrity check value (ICV (L1L2)) generated based on the license L1 and the license L2 is stored in them. The license 1 is justly stored in the media 2and the integrity check value (ICV (L1)) generated based on the license L1 is stored in them.

[0267]Supposing it copies {EKB and the license 2} which were stored in the media 1 to the media 2 in this compositionby the media 2. If a license check value is newly generatedICV (L1L2) will be generated andunlike Kicv (L1) stored in the media 2it will become clear that storing of the new license by an alteration or the unjust copy of a license was performed. In the device which reproduces mediaan ICV check is performed to the front step of regeneration stepsand coincidence of the generation ICV and the storing ICV is distinguishedand when not in agreementit becomes possible to prevent reproduction of a license of an illegal copy by having composition which does not perform reproduction.

[0268]In order to improve safetyit is good also as composition generated based on the data which rewrote the integrity check value (ICV) of the license and includes a counter. That isit has composition calculated by ICV=hash (Kicvcounter+1L1L2...). Hereone counter (counter+1) per rewriting of ICV is set up as a value to ∗∗∗∗∗∗∗∗∗∗∗∗∗. A counter value needs to have composition stored in a secure memory.

[0269]In the composition which cannot store the integrity check value (ICV) of a license in the same media as a licenseit is good also as composition which stores the integrity check value (ICV) of a license on media with an another license.

[0270]For examplewhen a license is stored in the media by which anti-copying policiessuch as the ReadOnly media and the usual MOare not takenIf an integrity check value (ICV) is stored in the same mediarewriting of ICV may be made by the inaccurate userand there is a possibility that the safety of ICV cannot be maintained. In such a caseby storing ICV in the safe media on a host machineand having composition which uses ICV for copy control (for examplecheck-in/check-outmove) of a licenseSafe management of ICV and the alteration check of a license are attained.

[0271]This example of composition is shown in <u>drawing 50</u>. The license 1 thru/or the license 3 are stored in the media 2201 from which anti-copying policiessuch as the ReadOnly media and the usual MOare not taken in <u>drawing 50</u>It is the example which stored the integrity check value (ICV) about these licenses in the safe media 2202 on the host machine with which it is not permitted that a user accesses freelyand prevented rewriting of the inaccurate integrity check value (ICV) by a user. If the device which equipped with the media 2201for example has PC which is a host machineand composition which performs the check of ICV in a server and judges reproductive propriety as such composition when it performs reproduction of the media 2201Reproduction of an unjust copy license or an alteration license can be

prevented.

[0272]The client to which this invention is applied can be used as PDA (Personal Digital Assistants)a portable telephonea game terminal machineetc. in addition to what is called a personal computer.

[0273]The computer by which the program which constitutes the software is included in hardware for exclusive use when performing a series of processings by softwareOr it is installed in the personal computer etc. which can perform various kinds of functionsfor exampleare general-purposeetc. from a network or a recording medium by installing various kinds of programs.

[0274]. As shown in <u>drawing 2</u>this recording medium is distributed apart from a device main frame in order to provide a user with a program. The magnetic disk 41 (a floppy disk is included) with which the program is recordedthe optical disc 42 (CD-ROM (Compact Disk - ReadOnly Memory).) . DVD (Digital Versatile Disk) is included. It is not only constituted by the package media which consist of the magneto-optical disc 43 (MD (Mini-Disk) is included) or the semiconductor memory 44butIt comprises ROM22 with which a user is provided in the state where it was beforehand included in the device main frame and on which the program is recordeda hard disk contained in the storage parts store 28etc.

[0275]In this Descriptioneven if the processing serially performed in accordance with an order that the step which describes the program recorded on a recording medium was indicated is not of course necessarily processed seriallyit also includes a parallel target or the processing performed individually.

[0276]In order for the program which performs processing relevant to security to prevent analyzing the processingit is desirable to encipher the program itself. For examplethe processing which performs cipher processing etc. can constitute the program as a tamper resistant module.

[0277]Since the license which carries out the utilization permission of the contents is specifiedthe information indicated to the header of contents may not be license ID which identifies a license uniquely. It is the information as which license ID specifies a license required for use of contents in above-mentioned working examplea certain license is the information which specifies the contents which permit useand it is the information which discriminates the license demanded by a license request from the client 1. The list of the various attribution information about the contents of contents is indicated to contentsand it may be made to indicate the conditional expression of the contents a utilization permission is carried out to a license by the license of. In this casethe attribution information included in contents is information which specifies the license to which use of those contents is permittedThe license is the information which specifies the contents which permit useand the conditional expression contained in a license serves as information from which license ID discriminates a license uniquely. When it does in this wayit becomes possible to match two or more licenses with one contentsand a license can be published flexibly.

[0278]In this Descriptiona system expresses the whole device constituted by two or more devices.
[0279]
[Effect of the Invention]According to the information processor of this invention and a methoda license serverand the programlike the above. It enables it to distribute the enciphered data freelyand by having enabled it to use contents by acquiring a license separatelywithout barring circulation of contentscopyright can be protected and a suitable usage fee can be collected.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a block diagram showing the composition of the contents providing system which applied this invention.
[Drawing 2]It is a block diagram showing the composition of the client of drawing 1.
[Drawing 3]It is a flow chart explaining the download processing of the contents of the client of drawing 1.
[Drawing 4]It is a flow chart explaining contents offer processing of the contents server of drawing 1.
[Drawing 5]It is a figure showing the example of the format in Step S26 of drawing 4.
[Drawing 6]It is a flow chart explaining contents playback processing of the client of drawing 1.
[Drawing 7]It is a flow chart explaining the details of the license acquisition processing of Step S43 of drawing 6.
[Drawing 8]It is a figure showing the composition of a license.
[Drawing 9]It is a flow chart explaining processing of license offer of the license server of drawing 1.
[Drawing 10]It is a flow chart explaining the details of the license update process in Step S45 of drawing 6.
[Drawing 11]It is a flow chart explaining the license update process of the license server of drawing 1.
[Drawing 12]It is a figure explaining the composition of a key.
[Drawing 13]It is a figure explaining a category node.
[Drawing 14]It is a figure showing the example of correspondence of a node and a device.
[Drawing 15]It is a figure explaining the composition of validation key blocks.
[Drawing 16]It is a figure explaining use of validation key blocks.
[Drawing 17]It is a figure showing the example of a format of validation key blocks.
[Drawing 18]It is a figure explaining the composition of the tag of validation key blocks.
[Drawing 19]It is a figure explaining the decoding processing of the contents using

DNK.

key.

[Drawing 48]It is a figure explaining other decoding processings of an ICV generation key.

[Drawing 49]It is a figure explaining management of the copy of the license by ICV.

[Drawing 50]It is a figure explaining management of a license.

[Description of Notations]

1-11-2 [A timer21CPUand 24 / An encryption decoding part25 codec partsand 26 / An input part27 outputting partsand 28 / A storage parts store and 29 / Communications department] A clientthe 2 Internetand 3 A contents server and 4 A license server5 fee-collection serverand 20